DOMAIN: SECURITY

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection – Desktop/Server

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

Baseline Environment (Current)

Desktop/Workstation

McAfee Anti Virus → McAfee
Trend Micro (Anti-virus) → Trend Micro
Norton Antivirus → Symantec (Norton)
CA eTrust → CA eTrust (inoculator)
F-Prot → Containment Targets
Sophos → Containment Targets

Tactical Deployment (2 Years)

McAfee
Trend Micro
Symantec (Norton)
CA eTrust (inoculator)

Strategic Direction (5 Years)

Those products that contain integrated anti-virus with centralized management.

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

McAfee, Trend Micro, Symantec (Norton), CA eTrust

Containment Targets

F-Prot, Sophos

Emerging Platforms

MS Windows Live OneCare

Implications and Dependencies

Independent of the perimeter virus protection. New signature files and signature updates must be kept current. Vendor must deliver consolidated management console.

Roadmap Notes

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection – Desktop/Server

- **Discipline Boundaries:**
  - To be used at the Desktop or on a Server. For, example virus protection running on the employee's desktop that scans the email prior to the email software opening the attached file.

- **Discipline Standards:**

- **Migration Considerations:**

- **Exception Considerations:**

- **Miscellaneous Notes:**
  - There are no virus protection protocols.

- **Established**
  - August 25, 2004

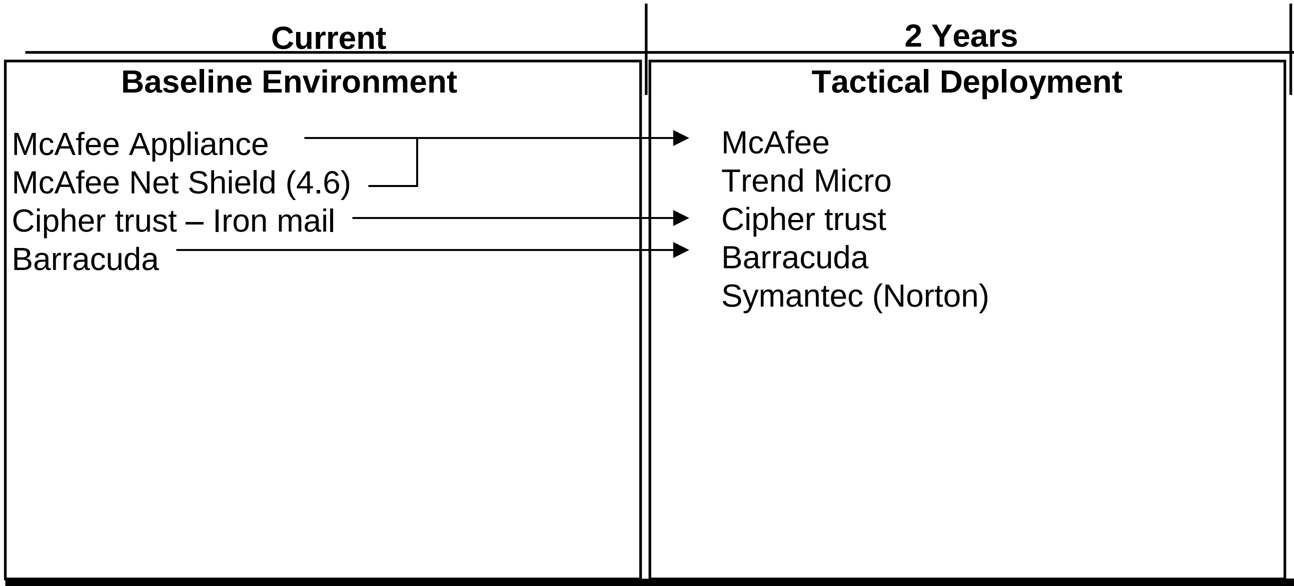
- **Date Last Updated:**
  - August 23, 2006

- **Next Review Date:**
  - August 2007

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection - Perimeter

DOMAIN: SECURITY



Current

Baseline Environment

McAfee Appliance
McAfee Net Shield (4.6)
Cipher trust – Iron mail
Barracuda

2 Years

Tactical Deployment

McAfee
Trend Micro
Cipher trust
Barracuda
Symantec (Norton)

5 Years

Strategic Direction

Market Watch

Additional functionality (e.g., spyware, antispam) included into perimeter packages

Shared	**Agency**
✓	✓

Retirement Targets

Mainstream Platforms (must be supported)

McAfee, Trend Micro, Symantec, Cipher Trust, Barracuda

Containment Targets

Emerging Platforms

Implications and Dependencies

Independent of the desktop/server virus protection. New signature files and signature updates must be kept current.
Vendor must deliver consolidated management console.

Roadmap Notes

DISCIPLINE: Host Protection

Discipline Roadmap for: Virus Protection - Perimeter

- **Discipline Boundaries:**
  - To be used as a perimeter device which refers to the logic position within the agencies network. For example, an email virus protection appliance where all email is scanned prior to being accessed by the employee's at their desktops.
- **Discipline Standards:**
- **Migration Considerations:**
- **Exception Considerations:**
- **Miscellaneous Notes:**
  - There are no virus protection industry protocols.
- **Established**
  - August 25, 2004
- **Date Last Updated:**
  - August 23, 2006
- **Next Review Date:**
  - August 2007

DISCIPLINE: Host Protection

Discipline Roadmap for: Anti-Spyware

DOMAIN: SECURITY

Current	2 Years	5 Years

Baseline Environment

Host-based

- Websense
- McAfee
- LavaSoft
- Microsoft
- Sunbelt
- Symantec
- PC Tools (unmanaged)
- Spybot Search and Destroy

Network-based

- LavaSoft
- Barracuda
- Intrusion Inc. (SpySnare)
- SonicWALL

Root Kit Defense

- Microsoft
- Backlight Defender

Tactical Deployment

Strategic Direction

Market watch for consolidated products.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

This market is poised for significant consolidation.

Implications and Dependencies

- Centralized management and administration of host-based clients.
- It is highly recommended that multiple products be used in concert in order to create an in-depth defense since not all products defend equally.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Host Protection

Discipline Roadmap for: Anti-Spyware

- **Discipline Boundaries:**
  - Spyware is a broad category of software designed to subvert a computer's operation for the benefit of a third party, without the informed consent of the owner. Spyware may be malicious in nature, intending to collect financial information for identify-theft or it can be relatively benign, originating form legitimate companies for the intended purpose of advertising. Anti-spyware is software that is designed to remove or block spyware.
- **Discipline Standards:**
  - Currently, there are no anti-spyware specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - Entities should consider restricting intentional downloading and installation of programs.
  - Entities should consider providing training to educate users in areas, such as:
    - Understanding of End User License Agreement (EULA), since often times agreements to install spyware are included in the fine print.
    - Proper response to pop-up windows.
    - Recognition of spyware symptoms.
    - Awareness of suspicious emails and "free" software.
  - Entities should consider tightening browser security, e.g. disabling Active X.
  - Entities should consider installing pop-up blockers.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DOMAIN: SECURITY

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: Email Protection (SPAM)

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
IronPort Systems Symantec McAfee Trend Micro Secure Computing (Cipher Trust) MicroSoft SonicWall Barracuda		Market Watch – Consolidation into a unified threat management device.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

This market is poised for significant consolidation.

Implications and Dependencies

- SonicWall and Barracuda are recommended for mid-size (1,000 units) and small enterprises.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: Email Protection (SPAM)

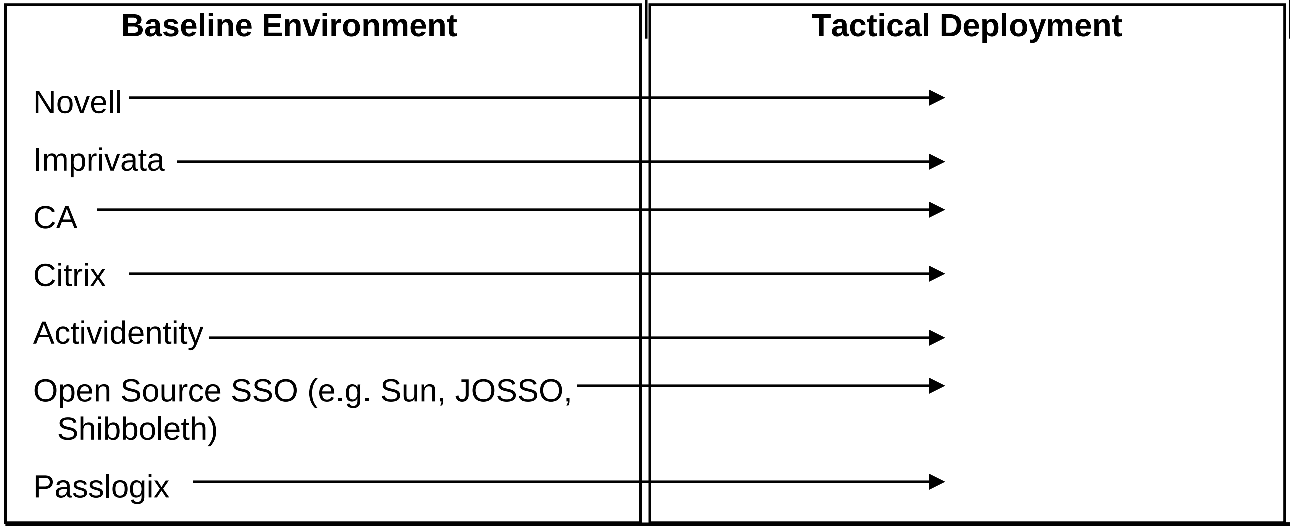
- **Discipline Boundaries:**
  - ❑ Spamming is the abuse of electronic messaging systems to send unsolicited, undesired, bulk messages. Email spam involves sending nearly identical messages to a few or millions of email recipients without permission. Spammers often harvest addresses from web pages, databases or by employing educated guessing.
- **Discipline Standards:**
  - ❑ Currently, there are no SPAM specific standards.
- **Migration Considerations:**
  - ❑ None
- **Exception Considerations:**
  - ❑ Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - ❑ None
- **Established**
  - ❑ November 15, 2006
- **Date Last Updated:**
  - ❑ November 15, 2006
- **Next Review Date:**
  - ❑ November 2007

DISCIPLINE: Identification and Authentication

Discipline Roadmap for: Enterprise Single Sign-On (ESSO)

DOMAIN: SECURITY

Current	2 Years	5 Years



Baseline Environment

Novell

Imprivata

CA

Citrix

Actividentity

Open Source SSO (e.g. Sun, JOSSO, Shibboleth)

Passlogix

Tactical Deployment

Strategic Direction

Market watch of ESSO and IAM (identity and access management) best practices and solutions.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Novell, Imprivata, CA, Citrix, Actividentity, Open Source SSO, Passlogix

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- User access and authorization through RDMS or LDAP based systems.
- Management through SNMPv3 or IP.

Roadmap Notes

- Standard to reviewed annually after adoption by the AOC.

DISCIPLINE: Identification and Authentication

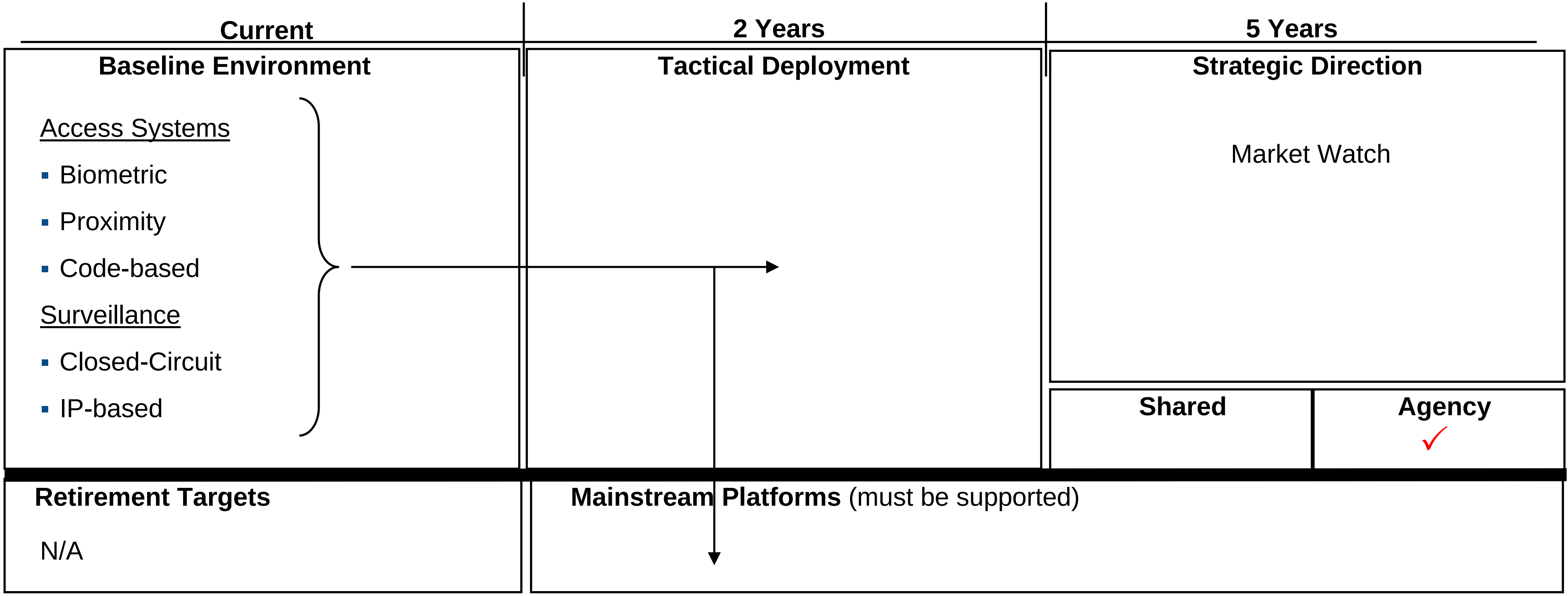
Discipline Roadmap for: Enterprise Single Sign-On (ESSO)

- **Discipline Boundaries:**
  - Enterprise Single Sign-On refers to specialized software that enables a user to authenticate once and gain access to multiple, often disparate, technology targets (e.g. network, web, and windows interfaces). ESSO is part of a larger segment of tools known as identity and access management (IAM), but it is differentiated from similar technologies (such as password wallets, password synchronization, and directory sign-on) because it is centrally administered on an enterprise level, provides automatic log on, and allows for legacy applications that are not directory-enabled.
- **Discipline Standards:**
  - Currently, there are no generally accepted independent standards. Instead, ESSO tools are proprietary, although some use XML as an integral part of their system. However, the Federal Government has adopted the Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) as its base standard.
- **Migration Considerations:**
  - Migration can be expensive and time consuming.
  - Positive ROI, through user and helpdesk time savings, is generally not realized unless an entity has several heterogeneous applications requiring daily sign-on with individualized credentials.
  - Can be coupled with other authentication methods, such as biometrics or smart cards, to provide stronger authentication in order to address concerns that a compromise of the master password likewise compromises all target systems.
  - Consider “webifying” legacy applications in order to exploit WAM (web access management) products as newer applications are usually natively web-enabled.
- **Exception Considerations:**
  - Specialized business needs requiring exception should to be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Facility Access and Monitoring Systems

DOMAIN: SECURITY



Current | 2 Years | 5 Years

Baseline Environment

Access Systems

- Biometric
- Proximity
- Code-based

Surveillance

- Closed-Circuit
- IP-based

Tactical Deployment

Strategic Direction

Market Watch

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- User access and authorization through database or LDAP based systems. Management through SNMPv3 or IP.
- Should be incorporated into the entity’s power redundancy strategy.

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.

DISCIPLINE: Physical & Environmental Protection

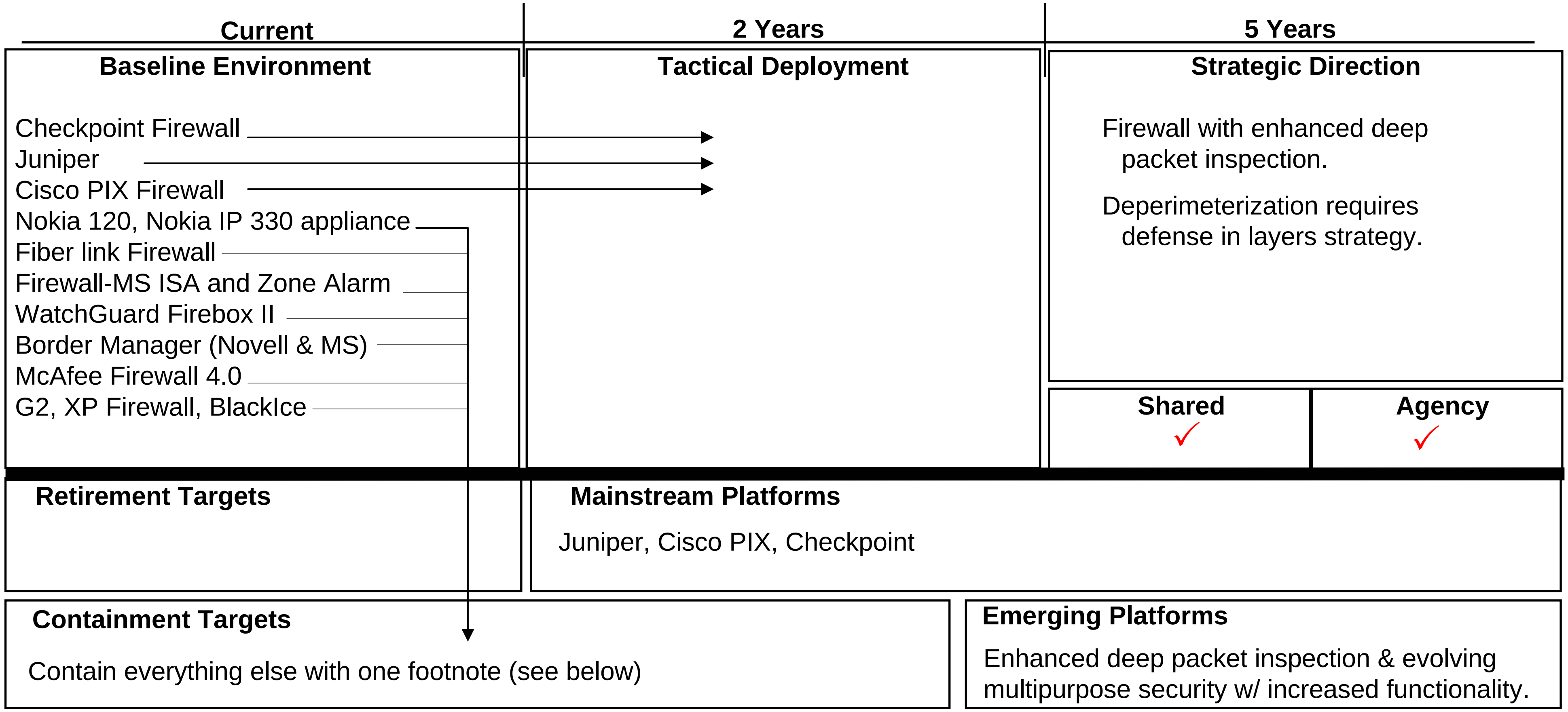
Discipline Roadmap for: Facility Access and Monitoring Systems

- **Discipline Boundaries:**
  - Barrier defense systems (e.g. key card, PIN entry, finger print biometrics, retinal scans, facial recognition, etc.) used to secure restricted access areas (e.g. server room, entity campus), as well as monitoring systems for surveillance (e.g. Closed Circuit TV). Does not address “boots on the ground” security personnel.
- **Discipline Standards:**
  - Must support the SC Enterprise Architecture standards for networking (e.g. LAN, WAN, cabling, etc.).
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - Should be implemented in a layered approach to provide failsafes:
    - Surveillance layer - e.g. cameras, motion detectors, and microphones
    - Access Control layer – e.g. key and keyless locks, biometrics, etc.
    - Infrastructure layer – e.g., windows, doors, locks, etc.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Firewalls

DOMAIN: SECURITY



Current

Baseline Environment

- Checkpoint Firewall
- Juniper
- Cisco PIX Firewall
- Nokia 120, Nokia IP 330 appliance
- Fiber link Firewall
- Firewall-MS ISA and Zone Alarm
- WatchGuard Firebox II
- Border Manager (Novell & MS)
- McAfee Firewall 4.0
- G2, XP Firewall, BlackIce

2 Years

Tactical Deployment

5 Years

Strategic Direction

Firewall with enhanced deep packet inspection.

Deperimeterization requires defense in layers strategy.

Shared	Agency
✓	✓

Retirement Targets

Mainstream Platforms

Juniper, Cisco PIX, Checkpoint

Containment Targets

Contain everything else with one footnote (see below)

Emerging Platforms

Enhanced deep packet inspection & evolving multipurpose security w/ increased functionality.

Implications and Dependencies

Deep packet inspection (DPI) is viewed as a must have feature because of the increasing blended attacks even in the tactical deployment. Perimeter firewalls that do not have DPI or limited DPI should be augmented with an intrusion prevention device.

Roadmap Notes

- Nokia H/W appliance running Checkpoint is valid for implementation.
- The committee plans to review this discipline yearly during August.

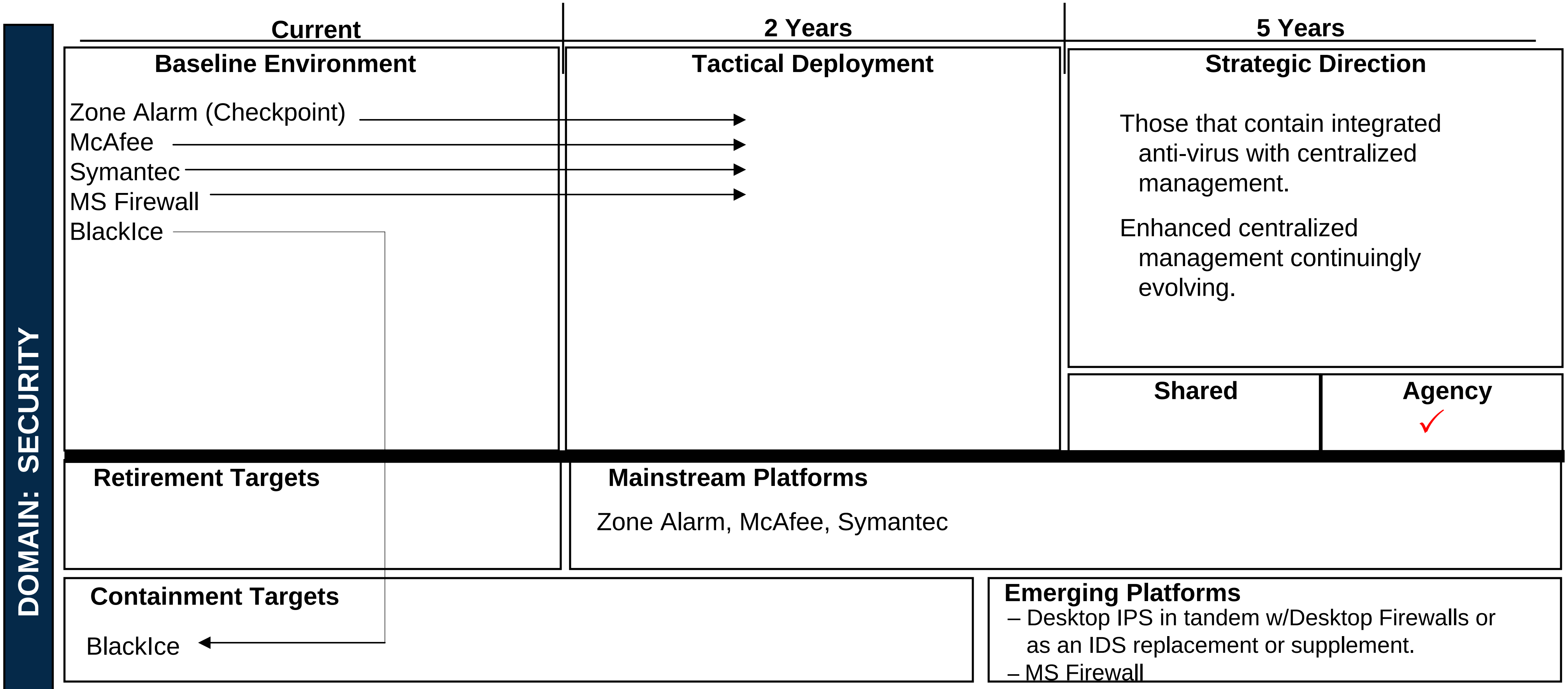
DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Firewalls

- **Discipline Boundaries:**
  - ❑ While separate disciplines, desktop firewalls and perimeter firewalls are not mutually exclusive of one another. The best implementation strategy would be a layered approach with a strong perimeter defense supplemented by a strong desktop defense. In many instances, you would model the firewall strategy after the evolution of the anti-virus strategy with at least a clear two tier approach. In some cases, additional firewalls or IPS implementations would be necessary to protect extremely sensitive data from both internal and external threats and to provide a third tier. Each implementation is situational with at least a deep packet inspection (DPI) perimeter solution.
- **Discipline Standards:**
- **Migration Considerations:**
  - ❑ Should an agency convert to a recommended firewall products, expect a price of $5K to $15K. This is the current price with deep packet inspection and VPN capabilities with four 10/100 network connections.
- **Exception Considerations:**
- **Miscellaneous Notes:**
- **Established Date**
  - ❑ April 28, 2004
- **Date Last Updated:**
  - ❑ August 23, 2006
- **Next Review Date:**
  - ❑ August 2007

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Desktop Firewalls



DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Zone Alarm (Checkpoint) → McAfee → Symantec → MS Firewall → BlackIce		Those that contain integrated anti-virus with centralized management. Enhanced centralized management continuingly evolving.

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms

Zone Alarm, McAfee, Symantec

Containment Targets

BlackIce

Emerging Platforms

- Desktop IPS in tandem w/Desktop Firewalls or as an IDS replacement or supplement.
- MS Firewall

Implications and Dependencies

Roadmap Notes

- The committee plans to review this discipline yearly during August.

DISCIPLINE: Network & Communications Protection

Discipline Roadmap for: Desktop Firewalls

- **Discipline Boundaries:**
  - ❑ While separate disciplines, desktop firewalls and perimeter firewalls are not mutually exclusive of one another. The best implementation strategy would be a layered approach with a strong perimeter defense supplemented by a strong desktop defense. In many instances, you would model the firewall strategy after the evolution of the anti-virus strategy with at least a clear two tier approach. In some cases, additional firewalls or IPS implementations would be necessary to protect extremely sensitive data from both internal and external threats and to provide a third tier. Each implementation is situational with at least a deep packet inspection (DPI) perimeter solution.

- **Discipline Standards:**

- **Migration Considerations:**

- **Exception Considerations:**

- **Miscellaneous Notes:**

- **Established Date**
  - ❑ April 28, 2004

- **Date Last Updated:**
  - ❑ August 23, 2006

- **Next Review Date:**
  - ❑ August 2007

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: HVAC (Heating, Ventilating, and Air Conditioning)

DOMAIN: SECURITY

Current	2 Years	5 Years	
Baseline Environment	**Tactical Deployment**	**Strategic Direction**	
Liebert →		Market Watch (green refrigerants and waterless refrigerants)	
Most data center purposed equipment for room, zone and rack level systems, supported by 24x7x365 support, are acceptable.		**Shared**	**Agency** ✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Liebert

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- Acquisition costs can be significant.
- External assessment recommended to determine capacity requirements. (Reference State Engineer’s Office existing contract)

Roadmap Notes

- Network-based power management systems must be secured with at least SNMPv3.

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: HVAC (Heating, Ventilating, and Air Conditioning)

- **Discipline Boundaries:**
  - HVAC specific to data center applications, may include rooftop units and distributed units that provide localized air cooling, or under-floor systems used in conjunction with raised floor areas.
- **Discipline Standards:**
  - ANSI 135 - BACnet Data Communication for Building Automation and Control Networks.
  - "Telecommunications Infrastructure Standard for Data Centers," TIA-942
- **Migration Considerations:**
  - Should be an integrated system that optimizes electrical power, space allocation and mechanical systems.
  - Strive for redundancy in the HVAC system by installing multiple units; focus on rack and tile placement to maximize the efficient flow of chilled air; use spot cooling as needed.
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - HVAC should be integrated with a humidity control system.
  - Design guidelines:
    - Ambient temperature should be between 70° and 72° F, with a relative humidity of 45% to 50%.
    - Redundant (distributed units) systems are better than centralized systems.
    - Design airflow to move from bottom to top and from front to back through racks to avoid consumption of used air.
    - Alternate cold-aisle and hot-aisle (intakes facing each other, exhaust facing each other) for temperature control efficiencies.
    - Establish a vapor barrier throughout the perimeter of the data center to minimize condensation.
    - Use spot cooling or special rack enclosures for hot spots in the data center layout.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Host Protection

Discipline Roadmap for: Host-based Intrusion Prevention System (HIPS)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

McAfee Entercept

Symantec

Cisco

ISS

Sana

AppArmor (Linux)

Strategic Direction

Market Watch of a single multi-function threat management client.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

McAfee Entercept, Symantec, Cisco, ISS, Sana, AppArmor

Containment Targets

N/A

Emerging Platforms

Consolidation into a single multi-function threat management client.

Implications and Dependencies

- Centralized management and administration of host-based clients.
- It is highly recommended that multiple products be used in concert in order to create an in-depth defense since not all products defend equally.

Roadmap Notes

- Certain products listed may be better suited for server or desktop dependent on use-case.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Host Protection

Discipline Roadmap for: Host-based Intrusion Prevention System (HIPS)

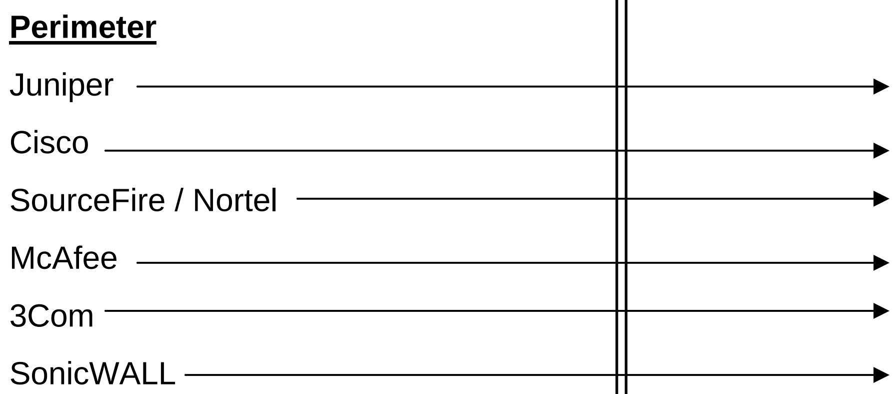
- **Discipline Boundaries:**
  - An IPS is any device which exercises control to protect networks, applications and computers from exploitation. IPS are intended to resolve ambiguities in passive network monitoring by placing detection in-line. There are 4 basic types of IPS: host-based network, content-based, and rate-based (the last 3 are addressed in a separate roadmap). Host-based IPS (HIPS) systems reside on a specific IP address, such as a PC system.
- **Discipline Standards:**
  - Currently, there are no HIPS specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: IPS (Intrusion Prevention System) / IDS (Intrusion Detection System)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**



Perimeter

Juniper

Cisco

SourceFire / Nortel

McAfee

3Com

SonicWALL

Strategic Direction

Market Watch of IPS / IDS merged within multifunctional security device, e.g. a firewall, security device.

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Juniper, Cisco, SourceFire / Nortel, McAfee, 3Com, SonicWall

Containment Targets

N/A

Emerging Platforms

IPS / IDS merged w/in multifunctional security device, e.g. a firewall, security device.

Implications and Dependencies

- Costs and implementation considerations can be substantial (~$30-$150k).
- SNMP v3

Roadmap Notes

- IDS still valid for asynchronous forensics.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Network Communications Protection

Discipline Roadmap for: IPS (Intrusion Prevention System) / IDS (Intrusion Detection System)

- **Discipline Boundaries:**
  - An IPS is any device which exercises control to protect networks, applications and computers from exploitation. IPS are intended to resolve ambiguities in passive network monitoring by placing detection in-line. There are 4 basic types of IPS: host-based (addressed in its own roadmap), network, content-based, and rate-based. Network IPS (NIPS) are designed to inspect traffic and can drop malicious traffic. Content-based IPS are designed to inspect network packets and can avoid infections and hacks. Rate-based IPS are designed to prevent denial of services attacks.
  - An IDS is a device which is used to detect all types of malicious network traffic and computer usage that can't be detected by conventional firewalls. An IDS differs from an IPS mainly in that it requires much more human involvement and is implemented near-line instead of in-line.
- **Discipline Standards:**
  - Currently, there are no IPS or IDS specific standards.
- **Migration Considerations:**
  - The biggest problem with IPS/IDS is false reports, either false positives (alerts w/o validity) or false negatives (no alerts when actual threats exist). Both problems are typically due to tuning issues, under or over tuning respectively. Because neither system can completely avoid false reports, it is recommended that tuning err towards false negatives, given the inherently greater consequences.
  - IDS tends to have higher manpower costs, while IPS tends to have functionality risks.
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Network Access Control (NAC)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
MS Cisco Juniper TCG ConSentry		Market Watch

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Containment Targets

N/A

Emerging Platforms

Market Watch

Implications and Dependencies

- None

Roadmap Notes

- Standard to be reviewed annually after adoption by the AOC.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Network Access Control (NAC)

- **Discipline Boundaries:**
  - None
- **Discipline Standards:**
  - None
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Power Management

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**

Baseline Environment

Desktop

- APC (Schneider Electric, SA)
- Tripp Lite

Data Center

- Battery-based
  - APC (Schneider Electric, SA)
  - Liebert
- Fly-wheel
  - Caterpillar
  - Pentadyne

Tactical Deployment

Strategic Direction

Market Watch

(DC Power Systems and "Green" Systems)

Shared	Agency
	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

Desktop: APC. Tripp Lite, Data Center: APC, Liebert, Caterpillar, Pentadyne

Containment Targets

N/A

Emerging Platforms

DC Power Systems, "Green" Systems

Implications and Dependencies

- Use backup generators for anticipated outages in excess of 20 minutes, UPS (uninterruptible power supply) for outage up to 20 minutes, and surge protection for unprotected systems.

Roadmap Notes

- Network-based power management systems must be secured with at least SNMPv3.

DISCIPLINE: Physical & Environmental Protection

Discipline Roadmap for: Power Management

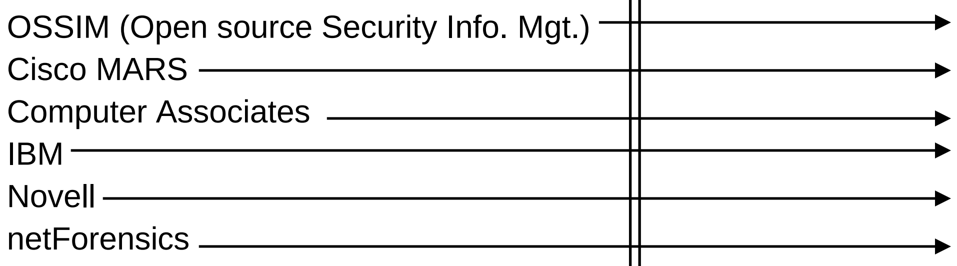
- **Discipline Boundaries:**
  - Redundant power sources specific to data center and desktop applications, including: uninterruptible power supply (UPS) and backup generators.
- **Discipline Standards:**
  - IEEE Emerald Book (data and electrical grounding)
  - IEEE Green Book (commercial grounding)
  - NEBS (Network Equipment Building Standards)
- **Migration Considerations:**
  - New data center designs should balance environmental efficiency with computing needs.
  - UPS should be sized to power 100% of “peak” load (or fault overload) of equipment until backup power kicks in.
- **Exception Considerations:**
  - Specialized business needs requiring exception should to be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - Typical needs range from 30 to 70 watts/ft.^{2} for computing equipment, plus additional power for HVAC, humidification, lighting and transformer losses.
  - Use the Uptime Institute’s fault tolerance levels for data centers to balance capital costs and service requirements:
    - Tier 1: Single path for power and cooling distribution; no redundant components - < 28.8 hours of downtime/year
    - Tier 2: Single path for power and cooling distribution; redundant components - < 22.0 hours of downtime/year
    - Tier 3: Multiple paths for power and cooling distribution; concurrently maintainable redundant components - < 1.6 hours of downtime/year
    - Tier 4: Multiple paths for power and cooling distribution; fault tolerant redundant components - < 0.4 hours of downtime/year
    - Tiers 3 & 4 (fault tolerant) will require backup generators.
  - Backup Generator considerations include:
    - Compliance with local fuel storage and noise abatement code.
    - Exhaust and vibration effects.
    - Maintenance and fuel contracts.
    - Plans for periodic testing.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Confidentiality and Integrity

Discipline Roadmap for: SIEM (Security Information & Event Management)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**



OSSIM (Open source Security Info. Mgt.)

Cisco MARS

Computer Associates

IBM

Novell

netForensics

Market Watch

Shared	Agency
✓	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

OSSIM, Cisco MARS, Computer Associates, IBM, Novell, netForensics

Containment Targets

N/A

Emerging Platforms

Market Watch - OSSIM

Implications and Dependencies

- Costs and implementation considerations can be substantial (~$30,000 - $150,000).

Roadmap Notes

- OSSIM – Low cost, fully functional Open source product for medium (1,000 units) and small enterprises.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Confidentiality and Integrity

Discipline Roadmap for: SIEM (Security Information & Event Management)

- **Discipline Boundaries:**
  - SIEM technology is composed of two basic capabilities: Security Information Management (SIM) and Security Event Management (SEM). SIM provides data analysis and reporting of historical events, often used to support regulatory requirements. SEM provides real-time data collection and correlation, often used to support incident response capabilities.
- **Discipline Standards:**
  - Currently, there are no SIEM specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - The South Carolina Information and Analysis Center (SC-ISAC) is an education and awareness initiative, jointly developed by the SC Joint Terrorism Task Force (JTTF), the State's Chief Information Office (CIO), the Federal Bureau of Investigation (FBI), and the US Secret Service (USSS). SC-ISAC's mission is to protect the State's citizenry and economy by safeguarding its critical information infrastructure. To that end, SC-ISAC offers a number of security services, including incident response and reporting. Therefore, State Agencies should contact SC-ISAC to develop an integrated incident response plan. Detailed information concerning SC-ISAC can be found on the WWW at http://secure.sc.gov, or by contacting the CIO's Director of Security Policy and Assessment at (803) 896-1660.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Virtual Private Networks

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
Checkpoint Cisco Nortel Juniper Symantec	Checkpoint Cisco Nortel Juniper	Secure Socket Layer (SSL) and IP Security protocol (IPSEC) Convergence towards TLS for security & access control

Shared	Agency
	✓

Retirement Targets

Mainstream Platforms (must be supported)

Cisco, Checkpoint, Nortel, Juniper

Containment Targets

Symantec

Emerging Platforms

Citrix Access Gateway (formerly Net 6), Transport Layer Security (TLS)

Implications and Dependencies

IPSEC often has network traversal vulnerabilities & therefore needs to be secured at the termination point with sufficient IDS capabilities.

Roadmap Notes

These recommendations are valid for IPSEC and SSL implementations.

DISCIPLINE: Network, Host Applications & Access Control

Discipline Roadmap for: Virtual Private Networks

- **Discipline Boundaries:**
  - Virtual Private Networks (VPN) are used to allow mobile users access to the corporate network from home or while they are traveling. Access is encrypted and controlled allowing only authorized users access to authorized resources.
  -
- **Discipline Standards:**
- **Migration Considerations:**
- **Exception Considerations:**
- **Miscellaneous Notes:**
- **Established**
  - August 25, 2004
- **Date Last Updated:**
  - August 23, 2006
- **Next Review Date:**
  - August 2007

State Information Technology Security Policy

1. **PURPOSE**

To establish a statewide security policy for the protection of Information Technology (IT) assets and resources for the State of South Carolina.

2. **SCOPE**

This Policy applies to agencies, departments, commissions, and boards (herein referred to as "agencies") that receive, expend or disburse State funds or incur obligations for the State. This policy does not apply to colleges and universities. However, they are encouraged to comply due to the frequent need to access and exchange data with the agencies.

The agency's assigned Designated Approving Authority (DAA), working in conjunction with the Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of statewide information technology policies, standards, and procedures within each agency.

3. **POLICY**

The State of South Carolina shall securely and economically protect its business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing Federal and State statutes pertaining to confidentiality, privacy, accessibility, availability, and integrity.

3.1. The policy establishes that:

- Agencies are responsible for providing security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of either 1) information collected or maintained by or on behalf of the Agency or 2) information systems used by an Agency or by a contractor of an Agency or other organization on behalf of the Agency.
- Agencies shall ensure that networks, hardware systems, and software application systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- Agencies shall ensure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in Agency software application systems.
- Levels of security applied to information systems and resources shall be commensurate with the value of the information being protected.
- Security controls applied to information systems and resources shall be sufficient to contain risk of loss or misuse of the information.
- Agencies are responsible for ensuring that information security management processes are integrated with Agency strategic and operational planning processes.

- Security architecture shall be based on industry-wide, open standards, and where possible, accommodate varying levels of security.
- Inter-Agency IT security components protecting critical Agency and State systems must be interoperable.
- Agencies are responsible for ensuring that staff is adequately trained in information security awareness.

3.2. Each Agency will have a comprehensive, documented set of policies that are periodically reviewed and updated. These policies address key security topic areas, including:

- Security strategy and management
- Security risk management
- Physical security
- System and network management
- System administration tools
- Monitoring and auditing
- Authentication and authorization
- Vulnerability management
- Encryption
- Security architecture and design
- Incident management
- Staff security practices
- Applicable laws and regulations
- Awareness and training
- Collaborative information security
- Contingency planning and disaster recovery

3.3. Agency shall assess their Technology Security by:

- Utilizing self assessments that adhere to industry-accepted best practices.
- Web-based reviews are offered by the CIO to ensure Agency compliance with best practices. Data from these reviews will be warehoused and accessible at the CIO.

Incident Management Best Practice

1. **PURPOSE**

   This policy defines agency responsibilities for responding to and reporting cyber intrusion and for sharing information related to potential incidents or threats with the South Carolina Information Sharing and Analysis Center (SC ISAC).

2. **SCOPE**

   This Policy applies to agencies, departments, commissions, and boards (herein referred to as "agencies") that receive, expend or disburse State funds or incur obligations for the State. This policy does not apply to colleges and universities. However, they are encouraged to comply due to the frequent need to access and exchange data with the agencies.

3. **POLICY**

   To secure and protect the South Carolina's critical information technology (IT) business processes and assets from cyber-crime or cyber-terrorism, State agencies should report all cyber intrusion to the SC ISAC. The agency's Assigned Designated Approving Authority (DAA), should appoint a coordinator to work with the SC ISAC.

4. **Cyber Intrusion:** Agencies should report any of the following acts by any person who, **without authority** or **acting in excess of authority**:

   - Accesses an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network.
   - Accesses, alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices.
   - Accesses, alters, damages, or destroys any computer application systems, programs, or data.
   - Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network.
   - Denies or causes the denial of IT-related services to any authorized user of those services.
   - Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person.
   - Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.
   - Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, or on behalf of the State, a political subdivision of the State, or a medical institution.

- Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network.
- Makes multiple attempts to access an IT device or network system within a brief period of time.

4.1. **Cyber Intrusion Reporting** – The agency should notify SC ISAC within one hour of detecting the intrusion by whatever means of communication is both available and fastest (i.e., phone, fax, e-mail, courier).

- The following information, at a minimum, is required when reporting intrusions to SC ISAC:

  a. Agency name
  b. The Agency SC ISAC Coordinator's name and phone number
  c. Brief description of intrusion and damages (real or anticipated)

- Whenever possible, the agency should capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder.

4.2. **SC ISAC Incident Report –** After notifying SC ISAC of the intrusion, the agency's coordinator should complete a SC ISAC Incident Report (see Attachment A) available from http://secure.sc.gov/site/Incident%20Reporting.asp. The agency's coordinator completing the report should provide as much detail as possible in the remarks fields and annotate the description of the intrusion with explanatory remarks. As more information becomes available or the situation changes, the agency's coordinator should revise and re-submit the incident report to SC ISAC with a clear date-time stamp.

4.3. **SC ISAC Activity –** Depending on the reported damage from the intrusion, SC ISAC will be in constant contact with the agency's coordinator at the affected agency, CIO, South Carolina Law Enforcement Division (SLED), Attorney General's Office, and other organizations, as necessary, until resolution and recovery efforts are completed.

4.4. **Alert Notifications**

4.4.4. **SC ISAC Responsibilities –** As SC ISAC creates or receives computer security alerts, it should determine whether to send it to "All Agencies" or specific Agencies, or only to specific individuals, depending on the security alert. Each alert should state, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk.

4.4.5. **Agency Responsibilities --** Upon receiving a SC ISAC Alert, agency SC ISAC Coordinators should notify agency personnel about the alert.

4.5. **SC ISAC Membership Form --** Agency SC ISAC Coordinators should complete a SC ISAC Membership Form (see Attachment B) and deliver it to SC ISAC. Agency SC ISAC Coordinators should ensure that the contact information on the form remains current and apprise SC ISAC of any changes.